Automating Collision Attacks on RIPEMD-160

Yingxin Li[1], Fukang Liu[2], Gaoli Wang[1]

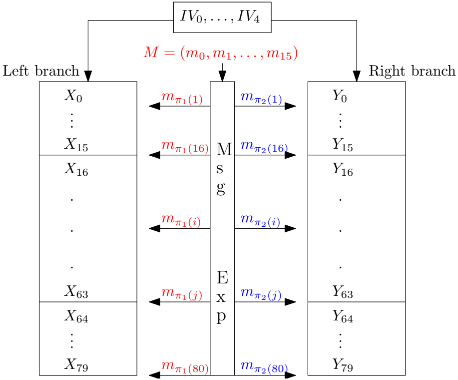
[1]East China Normal University, Shanghai, China
[2]Tokyo Institute of Technology, Tokyo, Japan

FSE 2024

Overview

RIPEMD-160

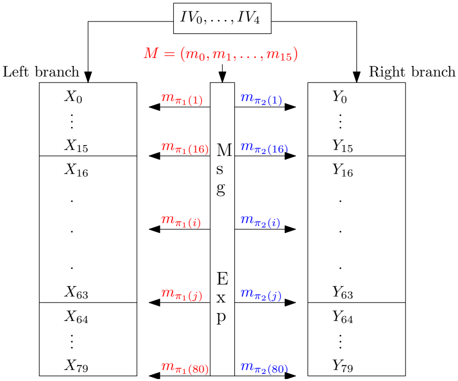
- FSE 1996 by Dobbertin et al.
- Strengthen MD5 (double branches, complex step function)
- ISO/IEC standard
- A famous application: Bitcoin



Step Function of RIPEMD-160

- Step function (left branch as an example)

$$
\begin{aligned}
Q_i &= X_{i-5} \lll 10 \boxplus F_i(X_{i-1}, X_{i-2}, X_{i-3} \lll 10) \boxplus m_{\pi(i)} \boxplus K_i, \\
X_i &= X_{i-4} \lll 10 \boxplus Q_i \lll s_i.
\end{aligned}
$$

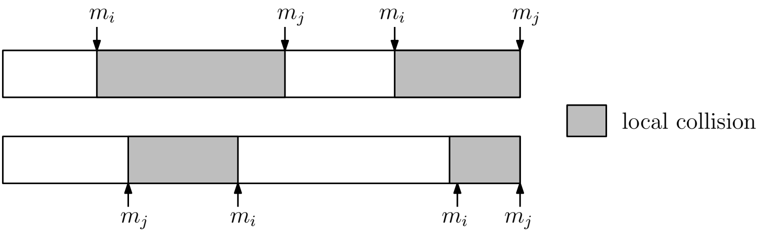


Revisiting Techniques for RIPEMD-160

- Known techniques and results
  - MILP-based tool to find differential trails (Eurocrypt 2023)
  - Collision attack up to 36 steps (Eurocrypt 2023)
  - Semi-free-start collision attack up to 40 steps (ToSC 2019)

Revisiting Techniques for RIPEMD-160

- Common procedure to mount (SFS) collision attacks
  - Fix the modular differences of message words $m_0 \ldots m_{15}$
  - Determine the places of local collisions
  - Find a valid solution of signed differences $(\Delta X_i, \Delta Y_i)$ such that a concrete differential trail leading to a collision can be constructed (easy with tools now)
  - Fulfill differential conditions (technical)



Revisiting Techniques for RIPEMD-160

- Example: 36-step collision attack (Eurocrypt 2023)
  - Inject proper differences at (m_0, m_6, m_9)
  - Determine local collisions

i	ΔX_i	$\pi_1(i)$	i	ΔY_i	$\pi_2(i)$
0	????????????????????????????????	0	0	================================	5
1	????????????????????????????????	1	1	================================	14
2	????????????????????????????????	2	2	================================	7
3	????????????????????????????????	3	3	????????????????????????????????	0
4	????????????????????????????????	4	4	????????????????????????????????	9
5	================================	5	5	????????????????????????????????	2
6	================================	6	6	????????????????????????????????	11
7	================================	7	7	????????????????????????????????	4
8	================================	8	8	????????????????????????????????	13
9	================================	9	9	????????????????????????????????	6
10	================================	10	10	????????????????????????????????	15
11	================================	11	11	????????????????????????????????	8
12	================================	12	12	????????????????????????????????	1
13	================================	13	13	????????????????????????????????	10
14	================================	14	14	????????????????????????????????	3
15	================================	15	15	????????????????????????????????	12
16	================================	7	16	????????????????????????????????	6
17	================================	4	17	????????????????????????????????	11
18	================================	13	18	????????????????????????????????	3
19	================================	1	19	????????????????????????????????	7
20	================================	10	20	????????????????????????????????	0
21	=======u==================u=====	6	21	????????????????????????????????	13
22	=======0==================0=====	15	22	????????????????????????????????	5
23	================1============1==	3	23	????????????????????????????????	10
24	================================	12	24	????????????????????????????????	14
25	================================	0	25	================================	15
26	================================	9	26	================================	8
27	================================	5	27	================================	12
28	================================	2	28	================================	4
29	================================	14	29	================================	9
30	================================	11	30	================================	1
31	================================	8	31	================================	2
32	================================	3	32	================================	15
33	================================	10	33	================================	5
34	================================	14	34	================================	1
35	================================	4	35	================================	3

Revisiting Techniques for RIPEMD-160

- Find a valid differential trail (left)

i	ΔX_i	$\pi_1(i)$	i	ΔY_i	$\pi_2(i)$
0	nuuuuuuuuuuuuuuuuu=nuuuuuuuuuuu=	0	0	================================	5
1	n===u=u==n=un====uuu=u=nn===u=uu	1	1	================================	14
2	=nun=u=n==n==nn==u==uun==nnu=un=	2	2	================================	7
3	====nu===========nu=============	3	3	????????????????????????????????	0
4	nnnnnnnn===unnnnnnnnnnnnnnnunnnn	4	4	????????????????????????????????	9
5	================================	5	5	????????????????????????????????	2
6	================================	6	6	????????????????????????????????	11
7	================================	7	7	????????????????????????????????	4
8	================================	8	8	????????????????????????????????	13
9	================================	9	9	????????????????????????????????	6
10	================================	10	10	????????????????????????????????	15
11	================================	11	11	????????????????????????????????	8
12	================================	12	12	????????????????????????????????	1
13	================================	13	13	????????????????????????????????	10
14	================================	14	14	????????????????????????????????	3
15	================================	15	15	????????????????????????????????	12
16	================================	7	16	????????????????????????????????	6
17	================================	4	17	????????????????????????????????	11
18	================================	13	18	????????????????????????????????	3
19	================================	1	19	????????????????????????????????	7
20	================================	10	20	????????????????????????????????	0
21	=======u==================u=====	6	21	????????????????????????????????	13
22	=======0==================0=====	15	22	????????????????????????????????	5
23	================1============1==	3	23	????????????????????????????????	10
24	================================	12	24	????????????????????????????????	14
25	================================	0	25	================================	15
26	================================	9	26	================================	8
27	================================	5	27	================================	12
28	================================	2	28	================================	4
29	================================	14	29	================================	9
30	================================	11	30	================================	1
31	================================	8	31	================================	2
32	================================	3	32	================================	15
33	================================	10	33	================================	5
34	================================	14	34	================================	1
35	================================	4	35	================================	3

Revisiting Techniques for RIPEMD-160

- Find a valid differential trail (right)

i	ΔX_i	$\pi_1(i)$	i	ΔY_i	$\pi_2(i)$
0	nuuuuuuuuuuuuuuuuu=nuuuuuuuuuuu=	0	0	================================	5
1	n===u=u==n=un====uuu=u=nn===u=uu	1	1	================================	14
2	=nun=u=n==n==nn==u==uun==nnu=un=	2	2	========0=====1============1====	7
3	====nu===========nu=============	3	3	====0=========1==n=========0==n1	0
4	nnnnnnnn===unnnnnnnnnnnnnnnunnnn	4	4	=10=n==0=======1=n1=101===1=0010	9
5	================================	5	5	=10=10=0010001=101000n0001110010	2
6	================================	6	6	10001nuunnnnnnnnnnnnnn=un1101110	11
7	================================	7	7	0u0n1uun00n10nu01nnun=nuuuuuuuuu	4
8	================================	8	8	n1un0nuuuu1=0u0un0unnnn1nn0nunuu	13
9	================================	9	9	=1=010u1000n00u01uu010n101=n100n	6
10	================================	10	10	u1=0u0110uu=u011=0=1=0=u1=1=0111	15
11	================================	11	11	111n==0=1=1=0n===11==10100n00==0	8
12	================================	12	12	==00==0=0===10==1=01=n0=1100===1	1
13	================================	13	13	==00=0==u==11===0n=1===1u===u01=	10
14	================================	14	14	==u==0===n===n==1========n===01=	3
15	================================	15	15	======u========1=0=uu====1=n==10	12
16	================================	7	16	===============n=1=============1	6
17	================================	4	17	==0====u=========1==1===========	11
18	================================	13	18	==1==========00=====1===========	3
19	================================	1	19	==========n==11=========n=======	7
20	================================	10	20	===nu=========================0=	0
21	=======u==================u=====	6	21	==========0===========01=0====1=	13
22	=======0==================0=====	15	22	====1=====1======0==u=11=1======	5
23	================1============1==	3	23	n===1=======nu===1==============	10
24	================================	12	24	=======u==============0===u=====	14
25	================================	0	25	======================1======0==	15
26	================================	9	26	=============================1==	8
27	================================	5	27	================================	12
28	================================	2	28	================================	4
29	================================	14	29	================================	9
30	================================	11	30	================================	1
31	================================	8	31	================================	2
32	================================	3	32	================================	15
33	================================	10	33	================================	5
34	================================	14	34	================================	1
35	================================	4	35	================================	3

Revisiting Techniques for RIPEMD-160

- Overall procedure to fulfilling differential conditions
  - Find a valid IV for the second message block with the first message block
  - Find a valid solution of $(X_i)_{0\leq i\leq 6}$ and $(Y_i)_{0\leq i\leq 9}$
  - Traverse valid (Y_{10}, Y_{11}) to fulfill conditions on (X_8, Y_{12})
  - Traverse valid Y_{13} to fulfill conditions on Y_{14}
  - Traverse valid Y_{15} to fulfill the remaining conditions

- Benefits
  - The number of conditions on $(X_i, Y_i,)_{i\geq 16}$ almost dominates the overall complexity to find the 36-step collision

Revisiting Techniques for RIPEMD-160

- Fulfill differential conditions

i	ΔX_i	$\pi_1(i)$	i	ΔY_i	$\pi_2(i)$
-5	10100101010010101101011111001000		-5	10100101010010101101011111001000	
-4	11101110001000000011110110000011		-4	11101110001000000011110110000011	
-3	11111010101100010100111101100010		-3	11111010101100010100111101100010	
-2	00011100010010000100111100010010		-2	00011100010010000100111100010010	
-1	00111011110101101010010000011111		-1	00111011110101101010010000011111	
0	nuuuuuuuuuuuuuuuu1nuuuuuuuuuuuu1	0	0	10111000110000010010000010111011	5
1	n010u0u11n1un0100uuu1u1nn000u1uu	1	1	11111101010011101100101101100001	14
2	1nun1u0n10n00nn10u10uun01nnu1un1	2	2	01101001000000101010110011010110	7
3	1011nu11111110010nu1110011100011	3	3	00100111110111101n001101000010n1	0
4	nnnnnnnn000unnnnnnnnnnnnnnnunnnn	4	4	0101n00001001001 1n10101010110010	9
5	11111110100000100000101011100010	5	5	010010100100011101000n0001110010	2
6	00110001111011101111011010111010	6	6	10001nuunnnnnnnnnnnnnn0un1101110	11
7	01101000000111101011001111000001	7	7	0u0n1uun00n10nu01nnun0nuuuuuuuuu	4
8	10011000010111000010010111111011	8	8	n1un0nuuuu110u0un0unnnn1nn0nunuu	13
9	01111100011111000110101010010100	9	9	110010u1000n00u01uu010n1010n100n	6
10	10000100100000000111100110011011	10	10	u100u0110uu0u0111001101u10100111	15
11	00000110100010001011100111011111	11	11	111n110011110n000110110100n00010	8
12	10100111100100110101011100111110	12	12	000001010010101110010n0111001111	1
13	10011000000000010001000010001011	13	13	10001011u11111010n010001u011u010	10
14	00011010101011010110100101110110	14	14	01u000011n010n01111001101n010010	3
15	00100001000111110011110010111100	15	15	101110u110100001101uu110010n0010	12
16	================================	7	16	110100101100111n0101101000001011	6
17	================================	4	17	0001101u110111011110111101011110	11
18	================================	13	18	10100001110000011100110111111110	3
19	================================	1	19	0111011100n1111001010011n0111111	7
20	================================	10	20	010nu010011000010100110010100101	0
21	=======u==================u=====	6	21	00001110010001011100110110011010	13
22	=======0==================0=====	15	22	0001101111101001101 0u11101001000	5
23	================1============1==	3	23	n===1=======nu===1==============	10
24	================================	12	24	=======u==============0===u=====	14
25	================================	0	25	======================1======0==	15
26	================================	9	26	=============================1==	8
27	================================	5	27	================================	12
28	================================	2	28	================================	4
29	================================	14	29	================================	9
30	================================	11	30	================================	1
31	================================	8	31	================================	2
32	================================	3	32	================================	15
33	================================	10	33	================================	5
34	================================	14	34	================================	1
35	================================	4	35	================================	3

Revisiting Techniques for RIPEMD-160

- Example: 40-step SFS collision attack (ToSC 2019)
  - Inject a proper nonzero difference at m_{12}
  - Deduce a sparse differential trail for $(\Delta Y_i)_{15 \leq i \leq 39}$
  - Find a compatible differential trail for $(\Delta X_i)_{12 \leq i \leq 39}$

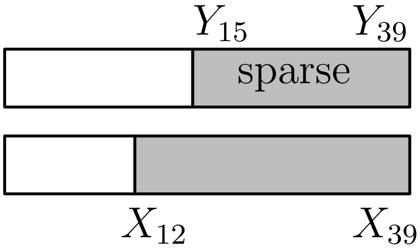
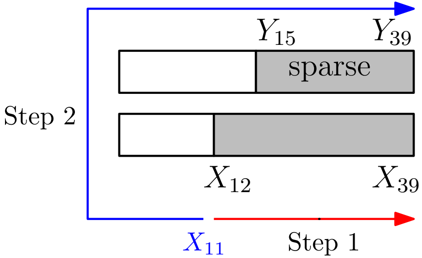


Figure: The shape of the 40-step differential trail

Revisiting Techniques for RIPEMD-160

- Fulfill differential conditions
  - Efficiently fulfill conditions on $(X_i)_{12 \leq i \leq 39}$
  - Traverse valid X_{11} to fulfill the remaining conditions



- Benefits
  - The number of conditions on the right branch (i.e., on Y_i) almost dominates the overall complexity to find the 40-step SFS collision

New Results for RIPEMD-160

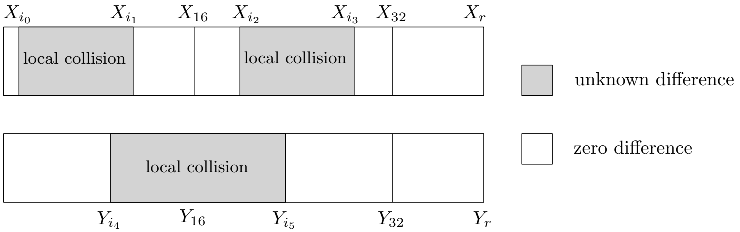
- Our new progress on the cryptanalysis of RIPEMD-160
  1. Re-implement the tool to find differential trails with SAT/SMT
  2. Find a practical collision attack on 40-step RIPEMD-160
  3. Propose SFS collision attacks on 41/42/43-step RIPEMD-160

New SAT/SMT-based Tools for RIPEMD-160

- SAT/SMT-based tool to find differential trails
  - Directly relies on the pseudo-code in Liu et al.'s paper (Eurocrypt 2023)
  - Use CNF (Conjunctive Normal Form) rather than linear inequalities to describe the constraints (i.e., propagation rules)
  - Enrich the available tools pool
- Our tool
  `https://github.com/Peace9911/ripemd160_attack.git`

New Collision Attack on 40-step RIPEMD-160

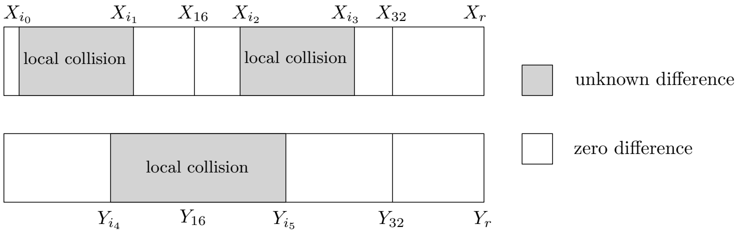
■ Observations from the 36-step collision attack (Eurocrypt 2023) where $i_0 = 0,\ i_1 = 9,\ i_2 = 21,\ i_3 = 26,\ i_4 = 3,\ i_5 = 29$.



- The first local collision spans from X_{i_0} to X_{i_1} where $i_0 < i_1 < 16$;
- The second local collision spans from X_{i_2} to X_{i_3} where $16 < i_2 < i_3 < 32$;
- The third local collision spans from Y_{i_4} to Y_{i_5} where $0 < i_4 < i_5 < 32$;

New Collision Attack on 40-step RIPEMD-160

- The ideas to improve the attack



  - The differential trail of the second local collision ($X_{i_2} \sim X_{i_3}$) should be sparse as it is an uncontrolled part;
  - The message words to inject differences should be used to update the internal states (X_i, Y_i) as late as possible where $i \geq 32$;

New Collision Attack on 40-step RIPEMD-160

- Three ways to construct the second local collision

message words	(i_2, i_3)	#conditions	r	#steps
(m_0, m_6, m_8, m_{11})	$(21, 31)$	8	37	38
$(m_0, m_2, m_{11}, m_{12})$	$(24, 30)$	8	39	40
(m_0, m_{12}, m_{13})	$(18, 25)$	44	41	42

New Collision Attack on 40-step RIPEMD-160

- Search for the 40-step differential trail

i	ΔX_i	$\pi_1(i)$	i	ΔY_i	$\pi_2(i)$
0	????????????????????????????????	0	0	================================	5
1	????????????????????????????????	1	1	================================	14
2	????????????????????????????????	2	2	================================	7
3	????????????????????????????????	3	3	????????????????????????????????	0
4	????????????????????????????????	4	4	????????????????????????????????	9
5	????????????????????????????????	5	5	????????????????????????????????	2
6	????????????????????????????????	6	6	????????????????????????????????	11
7	????????????????????????????????	7	7	????????????????????????????????	4
8	================================	8	8	????????????????????????????????	13
9	================================	9	9	????????????????????????????????	6
10	================================	10	10	????????????????????????????????	15
11	================================	11	11	????????????????????????????????	8
12	================================	12	12	????????????????????????????????	1
13	================================	13	13	????????????????????????????????	10
14	================================	14	14	????????????????????????????????	3
15	================================	15	15	????????????????????????????????	12
16	================================	7	16	????????????????????????????????	6
17	================================	4	17	????????????????????????????????	11
18	================================	13	18	????????????????????????????????	3
19	================================	1	19	????????????????????????????????	7
20	================================	10	20	????????????????????????????????	0
21	================================	6	21	????????????????????????????????	13
22	================================	15	22	????????????????????????????????	5
23	================================	3	23	????????????????????????????????	10
24	=========n======================	12	24	????????????????????????????????	14
25	==u======0======================	0	25	????????????????????????????????	15
26	==0============================1	9	26	????????????????????????????????	8
27	========================1=======	5	27	================================	12
28	================================	2	28	================================	4
29	================================	14	29	================================	9
30	================================	11	30	================================	1
31	================================	8	31	================================	2
32	================================	3	32	================================	15
33	================================	10	33	================================	5
34	================================	14	34	================================	1
35	================================	4	35	================================	3
36	================================	9	36	================================	7
37	================================	15	37	================================	14
38	================================	8	38	================================	6
39	================================	1	39	================================	9

New Collision Attack on 40-step RIPEMD-160

- Optimize the uncontrolled part on the right branch

i	ΔX_i	$\pi_1(i)$	i	ΔY_i	$\pi_2(i)$
0	????????????????????????????????	0	0	================================	5
1	????????????????????????????????	1	1	================================	14
2	????????????????????????????????	2	2	================================	7
3	????????????????????????????????	3	3	????????????????????????????????	0
4	????????????????????????????????	4	4	????????????????????????????????	9
5	????????????????????????????????	5	5	????????????????????????????????	2
6	????????????????????????????????	6	6	????????????????????????????????	11
7	????????????????????????????????	7	7	????????????????????????????????	4
8	================================	8	8	????????????????????????????????	13
9	================================	9	9	????????????????????????????????	6
10	================================	10	10	????????????????????????????????	15
11	================================	11	11	????????????????????????????????	8
12	================================	12	12	????????????????????????????????	1
13	================================	13	13	????????????????????????????????	10
14	================================	14	14	????????????????????????????????	3
15	================================	15	15	=========n==============n=======	12
16	================================	7	16	=============================u==	6
17	================================	4	17	================================	11
18	================================	13	18	================================	3
19	================================	1	19	=====================0==========	7
20	================================	10	20	=====================1==========	0
21	================================	6	21	===========u====================	13
22	================================	15	22	================================	5
23	================================	3	23	===========1====================	10
24	=========n======================	12	24	===========1=============010000=	14
25	==u======0======================	0	25	=u=======================111111=	15
26	==0============================1	9	26	===============nuuuuu===========	8
27	========================1=======	5	27	======1=========================	12
28	================================	2	28	======0=========================	4
29	================================	14	29	================================	9
30	================================	11	30	================================	1
31	================================	8	31	================================	2
32	================================	3	32	================================	15
33	================================	10	33	================================	5
34	================================	14	34	================================	1
35	================================	4	35	================================	3
36	================================	9	36	================================	7
37	================================	15	37	================================	14
38	================================	8	38	================================	6
39	================================	1	39	================================	9

New Collision Attack on 40-step RIPEMD-160

- The full 40-step differential trail

i	ΔX_i	$\pi_1(i)$	i	ΔY_i	$\pi_2(i)$
0	unnn============================	0	0	================================	5
1	===============nuuuu=n==========	1	1	================================	14
2	u=uun=u==========n==u====un=nnnn	2	2	=============0==================	7
3	=====nnn===unun==u==u====nn=====	3	3	0==u============================	0
4	u=u==uu==u==================n=nu	4	4	0====1===========0==1=n==1===010	9
5	============nuuu=n======u=n======	5	5	101====u==0=00=1===0000=100u0000	2
6	==u====nuu======================	6	6	0110=1===nnuu1nuuuuuuuuuu10100=0	11
7	================unnnnnnnnnn=====	7	7	1unnnnn11000unn00unn10nunn11=110	4
8	================================	8	8	=1011nu001nu111nuu=unnn0101nuuuu	13
9	================================	9	9	00u==nu00u010===1000101u=0101n0=	6
10	================================	10	10	111====0==u=n10=0u01=1n01=010==1	15
11	================================	11	11	0=0=n1=0=10n0===u====n1=1===0===	8
12	================================	12	12	11u===10=0=1u=0======1==0=1u===0	1
13	================================	13	13	==0======1==0=n=10=0====1=10===n	10
14	================================	14	14	==1====0========u1=1===========u	3
15	================================	15	15	=======1=n==============n=======	12
16	================================	7	16	=============================u==	6
17	================================	4	17	================================	11
18	================================	13	18	================================	3
19	================================	1	19	=====================0==========	7
20	================================	10	20	=====================1==========	0
21	================================	6	21	===========u====================	13
22	================================	15	22	================================	5
23	================================	3	23	===========1====================	10
24	=========n======================	12	24	===========1=============010000=	14
25	==u======0======================	0	25	=u=======================111111=	15
26	==0=============================1	9	26	===============nuuuuu===========	8
27	========================1=======	5	27	======1=========================	12
28	================================	2	28	======0=========================	4
29	================================	14	29	================================	9
30	================================	11	30	================================	1
31	================================	8	31	================================	2
32	================================	3	32	================================	15
33	================================	10	33	================================	5
34	================================	14	34	================================	1
35	================================	4	35	================================	3
36	================================	9	36	================================	7
37	================================	15	37	================================	14
38	================================	8	38	================================	6
39	================================	1	39	================================	9

New Collision Attack on 40-step RIPEMD-160

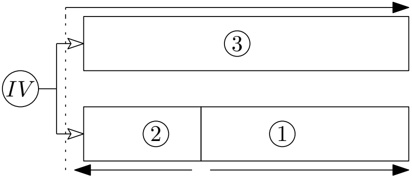
Find a colliding message pair in about 16 hours with 115 threads!

Table: The colliding message pair (M_0, M_1) and (M_0, M_1') for 40-step RIPEMD-160

M_0	4b1de304	f52a5a3e	bbd7d814	6454a1d6	a5571007	6c4151f5	8970f768	32c48fd1
	54c428ea	113b00cf	3db1bb85	1d2b2de6	89157118	89157118	d22f990b	6db9f321
M_1	0a179ed0	582e9fee	8c68cd3d	0d120a6e	de43af57	df2e7a6f	2b40967e	df302947
	ee7f066f	d7b7707d	9f1cc8a9	eaecfcb8	0b449f1a	ec058b69	996ee0d2	994ef6b1
M_1'	0a159ed0	582e9fee	8c48cd3d	0d120a6e	de43af57	df2e7a6f	2b40967e	df302947
	ee7f066f	d7b7707d	9f1cc8a9	eaecfd38	0b451f1a	ec058b69	996ee0d2	994ef6b1
hash	a76b7982	e39826f9	52eb6b63	6b48ecdd	4ddca6c5			

New SFS Collision Attack on 41/42/43-step RIPEMD-160

- Observations from the 40-step SFS collision attack (ToSC 2019)



1. The differential probability on the right branch ③ almost affects the overall time complexity;
2. The right-branch differential trails were deduced by hand;
3. Constructing a sparser right-branch differential trail may bring improved attacks.

- Optimizing the sparsity of a trail is easy with MILP/SAT/SMT

New SFS Collision Attack on 41/42/43-step RIPEMD-160

- Example: search for the 43-step differential trail

i	ΔX_i	$\pi_1(i)$	i	ΔY_i	$\pi_2(i)$
0	================================	0	0	================================	5
1	================================	1	1	================================	14
2	================================	2	2	================================	7
3	================================	3	3	================================	0
4	================================	4	4	================================	9
5	================================	5	5	================================	2
6	================================	6	6	================================	11
7	================================	7	7	================================	4
8	================================	8	8	================================	13
9	================================	9	9	================================	6
10	================================	10	10	================================	15
11	================================	11	11	================================	8
12	????????????????????????????????	12	12	================================	1
13	????????????????????????????????	13	13	================================	10
14	????????????????????????????????	14	14	================================	3
15	????????????????????????????????	15	15	????????????????????????????????	12
16	????????????????????????????????	7	16	????????????????????????????????	6
17	????????????????????????????????	4	17	????????????????????????????????	11
18	????????????????????????????????	13	18	????????????????????????????????	3
19	????????????????????????????????	1	19	????????????????????????????????	7
20	????????????????????????????????	10	20	????????????????????????????????	0
21	????????????????????????????????	6	21	????????????????????????????????	13
22	????????????????????????????????	15	22	????????????????????????????????	5
23	????????????????????????????????	3	23	????????????????????????????????	10
24	????????????????????????????????	12	24	????????????????????????????????	14
25	????????????????????????????????	0	25	????????????????????????????????	15
26	????????????????????????????????	9	26	????????????????????????????????	8
27	????????????????????????????????	5	27	????????????????????????????????	12
28	????????????????????????????????	2	28	????????????????????????????????	4
29	????????????????????????????????	14	29	????????????????????????????????	9
30	????????????????????????????????	11	30	????????????????????????????????	1
31	????????????????????????????????	8	31	????????????????????????????????	2
32	????????????????????????????????	3	32	????????????????????????????????	15
33	????????????????????????????????	10	33	????????????????????????????????	5
34	????????????????????????????????	14	34	????????????????????????????????	1
35	????????????????????????????????	4	35	????????????????????????????????	3
36	????????????????????????????????	9	36	????????????????????????????????	7
37	????????????????????????????????	15	37	????????????????????????????????	14
38	????????????????????????????????	8	38	????????????????????????????????	6
39	????????????????????????????????	1	39	????????????????????????????????	9
40	????????????????????????????????	2	40	????????????????????????????????	11
41	????????????????????????????????	7	41	????????????????????????????????	8
42	????????????????????????????????	0	42	????????????????????????????????	12

New SFS Collision Attack on 41/42/43-step RIPEMD-160

- Minimize the hamming weight on the right branch

i	ΔX_i	$\pi_1(i)$	i	ΔY_i	$\pi_2(i)$
0	================================	0	0	================================	5
1	================================	1	1	================================	14
2	================================	2	2	================================	7
3	================================	3	3	================================	0
4	================================	4	4	================================	9
5	================================	5	5	================================	2
6	================================	6	6	================================	11
7	================================	7	7	================================	4
8	================================	8	8	================================	13
9	================================	9	9	================================	6
10	================================	10	10	================================	15
11	================================	11	11	================================	8
12	????????????????????????????????	12	12	================================	1
13	????????????????????????????????	13	13	====================0===========	10
14	????????????????????????????????	14	14	====================1===========	3
15	????????????????????????????????	15	15	==========n=====================	12
16	????????????????????????????????	7	16	================================	6
17	????????????????????????????????	4	17	==========1=====================	11
18	????????????????????????????????	13	18	==========1=====================	3
19	????????????????????????????????	1	19	u===============================	7
20	????????????????????????????????	10	20	================================	0
21	????????????????????????????????	6	21	1==============================0	13
22	????????????????????????????????	15	22	1==============================1	5
23	????????????????????????????????	3	23	=====================un=========	10
24	????????????????????????????????	12	24	================================	14
25	????????????????????????????????	0	25	====================001=========	15
26	????????????????????????????????	9	26	====================111=========	8
27	????????????????????????????????	5	27	==========nnn===================	12
28	????????????????????????????????	2	28	================================	4
29	????????????????????????????????	14	29	============1===================	9
30	????????????????????????????????	11	30	==1=============================	1
31	????????????????????????????????	8	31	==u=============================	2
32	????????????????????????????????	3	32	==1=============================	15
33	????????????????????????????????	10	33	==1======0======================	5
34	????????????????????????????????	14	34	=========n==============1=======	1
35	????????????????????????????????	4	35	=========1==============u=======	3
36	????????????????????????????????	9	36	=========1==============10======	7
37	????????????????????????????????	15	37	========0================u=====1	14
38	????????????????????????????????	8	38	========n=====0==========1=====n	6
39	????????????????????????????????	1	39	===0====1====1u======1====1===11	9
40	????????????????????????????????	2	40	===u====0=====1=10===0========0=	11
41	????????????????????????????????	7	41	===0====n=======uu==============	8
42	????????????????????????????????	0	42	=====================n=========n	12

New SFS Collision Attack on 41/42/43-step RIPEMD-160

- The full 43-step differential trail

i	ΔX_i	$\pi_1(i)$	i	ΔY_i	$\pi_2(i)$
0	================================	0	0	================================	5
1	================================	1	1	================================	14
2	================================	2	2	================================	7
3	================================	3	3	================================	0
4	================================	4	4	================================	9
5	================================	5	5	================================	2
6	================================	6	6	================================	11
7	================================	7	7	================================	4
8	================================	8	8	================================	13
9	================================	9	9	================================	6
10	================================	10	10	================================	15
11	================================	11	11	================================	8
12	==========n=====================	12	12	================================	1
13	==nu============================	13	13	====================0===========	10
14	=n========0===============u=====	14	14	====================1===========	3
15	10=0==============u=====110n====	15	15	==========n=====================	12
16	u1==============1=0====1=1=0====	7	16	================================	6
17	0=======1====1===11====0=n=1====	4	17	==========1=====================	11
18	1==1====0========0====1n=0======	13	18	==========1=====================	3
19	===u====u======1=n0===00=1======	1	19	u===============================	7
20	===0====0====1=0=1====u1========	10	20	================================	0
21	=======1n====1=n=1====0==1====1=	6	21	1==============================0	13
22	=======01===1n=0===0==1=====0===	15	22	1==============================1	5
23	=====1=n10==00=1==0===========0=	3	23	=====================un=========	10
24	===1=0=0=n==u=====u===========0=	12	24	================================	14
25	=010=n11=0==0===10111010000101n=	0	25	====================001=========	15
26	==1==1011000011010100=1110=00010	9	26	====================111=========	8
27	100=00nuuuuuuuuuuuuuu11uuu0uun00	5	27	==========nnn===================	12
28	10u1nn1n0n00u0nu1u01110100=uun=1	2	28	================================	4
29	un1000u1000nnu10u01nuunuu0=11u1n	14	29	============1===================	9
30	1110n10n=1n1001u010100011n0000=n	11	30	==1=============================	1
31	1101110u=0000100===0=u=0010==0=0	8	31	==u=============================	2
32	1=0=01=1===1u0=0===u=0==uu1=11=u	3	32	==1=============================	15
33	0=n0=n1=0==01u11==110==000u=u0=0	10	33	==1======0======================	5
34	==10=u==n1==01u0==u=u110u101u=1=	14	34	=========n==============1=======	1
35	0=n=11==1011=n1=1=n=10n=1u=0n=11	4	35	=========1==============u=======	3
36	1=010=0=1=0n00u===00u=1=10==1=uu	9	36	=========1==============10======	7
37	===0==n=0110n=1===0=1=n=0=====10	15	37	========0================u=====1	14
38	==1===1=1u0=1=======0=0=====1==u	8	38	========n=====0==========1=====n	6
39	==0=====u1====0=============0==u	1	39	===0====1====1u======1====1===11	9
40	========1=====n======1===0====10	2	40	===u====0=====1=10===0========0=	11
41	==============1======0===n====0=	7	41	===0====n=======uu==============	8
42	========u=======nn==============	0	42	=====================n=========n	12

Summary and Problems

- Summary
  - A SAT/SMT-based tool for RIPEMD-160
  - The first practical and best collision attack on RIPEMD-160
  - The best semi-free-start collision attack on RIPEMD-160

Attack type	Steps (80 in total)	Time	Memory	References
SFS collision	48*	$2^{76.5}$	2^{64}	ToSC 2017
	40	$2^{74.6}$	*negligible*	ToSC 2019
	41	$2^{59.7}$	*negligible*	Ours
	42	$2^{67.3}$	*negligible*	Ours
	43	$2^{74.8}$	*negligible*	Ours
collision	34	$2^{74.3}$	2^{32}	CRYPTO 2019
	36	$2^{64.5}$	*negligible*	Eurocrypt 2023
	40	*practical*	*negligible*	Ours

* An attack starts at an intermediate step.

Summary and Problems

- Problem
  - Are there other ways to construct local collisions such that the (SFS) collision attacks on RIPEMD-160 can be further improved?

Overview of the modelling method

- The step function

$$d_{i+5} = (d_{i+1}^{\lll 10}) \boxplus (F(d_{i+4}, d_{i+3}, d_{i+2}^{\lll 10}) \boxplus (d_i^{\lll 10}) \boxplus m \boxplus c_i)^{\lll s},$$

- Simplification (rotation ($\lll 10$) does not matter)

$$a_5 = a_1 \boxplus (F(a_4, a_3, a_2) \boxplus a_0 \boxplus m \boxplus c)^{\lll s}.$$

- Decomposition

$$\begin{aligned} b_0 &= m \boxplus c, \\ b_1 &= F(a_4, a_3, a_2), \\ b_2 &= b_0 \boxplus b_1, \\ b_3 &= b_2 \boxplus a_0, \\ b_4 &= b_3^{\lll s}, \\ b_5 &= a_1 \boxplus b_4, \\ a_5 &= b_5. \end{aligned}$$

Overview of the modelling method

- Liu et al.'s idea (Eurocrypt 2023):
  - Model the deterministic signed difference addition for $z = x \boxplus y$, i.e.,

$$(\Delta x, \Delta y) \rightarrow \Delta z$$

  - Model the signed difference transitions for the Boolean function F, i.e.

$$(\Delta a_4, \Delta a_3, \Delta a_2) \rightarrow \Delta b_1$$

  - Model the expansion of the modular difference, i.e., finding all Δz from a fixed $\Delta z'$ such that they correspond to the same modular difference, i.e.,

$$\Delta z' \rightarrow \Delta z$$

  - Model the update $a_5 = a_1 \boxplus b_3^{\lll s}$, i.e.,

$$(\Delta a_1, \Delta b_3) \rightarrow \Delta a_5$$